K

Uso de técnicas de *fingerprinting* en el sitio de la campaña de Miguel Uribe Turbay

En el *Pequeño Manual* hablamos del uso de técnicas de *fingerprinting* por parte del candidato Miguel Uribe. Así, en los flujos HTTP(S) generados desde su página principal, se pudo encontrar el siguiente paquete HTTPS que envía una solicitud al subdominio `marketing.migueluribeturbay.co`.

Observamos que se solicita una imagen ficticia con el nombre explícito `mtracking.gif` y envía en los parámetros de la url una serie de información sobre el usuario, incluyendo características técnicas de nuestro equipo (resolución de pantalla, zona de tiempo, sistema operativo, etc.) y una variable llamada `fingerprint` que contiene un número de identificación hexadecimal. Es decir, la propia solicitud de imagen incluye diversos datos de nuestro equipo.

La solicitud también transmite varias *cookies* asociadas al servicio Mautic y, en la respuesta, el servidor web modifica el valor de una de ella (`mautic_referer_id`).

[SOLICITUD]

```
https://marketing.migueluribeturbay.co/mtracking.gif?page_
title=Inicio%20%7C%20Miguel%20Uribe%20Turbay&page_
language=es-CL&page_referrer=www.migueluribeturbay.
co&page_url=https%3A%2F%2Fwww.migueluribeturbay.co%2F%3Fcn-
reloaded%3D1&counter=0&resolution=1280x720&timezone_offset=300&
platform=Linux%20x86_64&do_not_ track=unspecified&adblock=
false&fingerprint=8785309d593003dc0221dd48f037a5b9

GET
/mtracking.gif?page_title=Inicio%20%7C%20Miguel%20Uribe%20
Turbay&page_language=es-CL&page_referrer=www.migueluribeturbay.
co &page_url=https%3A%2F%2F www.migueluribeturbay.co%2F%3Fcn-
reloaded%3D1& counter=0&resolution=1280x720& timezone_
offset=300& platform=Linux%20x86_64&do_not_track=unspecified&
adblock=false&fingerprint=8785309d593003dc0221dd48f037a5b9 HTTP/1.1
Host: marketing.migueluribeturbay.co
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: es-CL,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://www.migueluribeturbay.co/?cn-reloaded=1
```

```
Cookie: 539f581af2ac98b32c119d8ef1881172=tqi9djdfunaoih66rlpopjg5lp;
nvg56903=9d1585ebc7829b43a6b7e783909|2_259; _
ga=GA1.2.556694798.1568591455; _gid=GA1.2.660391297.1568591455;
mautic_device_id=a6vug7i9r3qtgqzss97v806; mtc_
id=56206; mtc_sid=a6vug7i9r3qtgqzss97v806;
mautic_session_id=a6vug7i9r3qtgqzss97v806;
a6vug7i9r3qtgqzss97v806=56206;
mautic_referer_id=85158; __utma=21743527. 556694798.
1568591455. 1568591462.1568591462.1; __utmb=21743527. 1.9.
1568591462; __utmc=21743527; __utmz=21743527.1568591462.1.1.
utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
_dc_gtm_UA-143424543-1=1
Connection: keep-alive
```

[RESPUESTA DEL SERVIDOR]

```
HTTP/1.1 200 OK
Date: Sun, 15 Sep 2019 23:55:09 GMT
Server: Apache/2.4.29 (Ubuntu)
Set-Cookie: mautic_referer_id=85166; expires=Mon, 16-
Sep-2019 00:25:09 GMT; Max-Age=1800; path=/; secure
Cache-Control: no-cache=Set-Cookie, private, proxy-revalidate
Content-Encoding: none
Connection: close
Content-Length: 42
Expires: Wed, 11 Jan 2000 12:59:00 GMT
Last-Modified: Wed, 11 Jan 2006 12:59:00 GMT
Pragma: no-cache
Content-Type: image/gif
```

Fundación Karisma

<K+LAB>

INDELA